Notice of Allowability	Application No.	Applicant(s)	
	09/648,211	FLOWERS ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/15/05*.

2. ☒ The allowed claim(s) is/are *2,29,44 and 46-48*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER
3/17/06

DETAILED ACTION

1. This is in response to the RCE filed on 15 December 2005.

2. Claims 2, 29, 44 and 46-48 are pending in the application.

3. Claims 2, 29, 44 and 46-48 have been allowed.

4. Claims 1, 3-28, 30-43, 45 and 49 have been cancelled.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Dorian Cartwright on 3 March 2006.

The application has been amended as follows:

1. (Cancelled)

2. (Currently amended) The method of claim 44 [[1]], wherein:

identifying the [[an]] operating system includes sending the [[a]] first set of packets to the remote host and receiving a second set of packets from the remote host in response to the first set of packets, and analyzing the second set of packets for inferential information indicative of the operating system; and

identifying the [[a]] service includes sending the [[a]] third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to the third set of packets, wherein information contained in the third set of packets is

based on information received in the second set of packets, and analyzing the fourth set of packets for inferential information indicative of the service.

3-28. (Cancelled)

29. (Currently amended) A method of detecting a vulnerability of a network, comprising: ~~The method of claim 26, wherein:~~

sending a first set of test packets to a remote host on the network;

receiving a first set of reflexive packets from the remote host in response to the first set of test packets, at least part of the first set of reflexive packets including header information that is unique to an operating system;

inferring the operating system;

sending a second set of test packets to the remote host;

receiving a second set of reflexive packets from the remote host in response to the second set of test packets, at least part of the second set of reflexive packets including header information that is unique to a service; and

inferring the service,

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service,

wherein the first set of test packets includes:

a SYN Packet with false flag in the TCP option header;

a Fragmented UDP packet with malformed header (any header inconsistency is sufficient), where the packet is 8K in size;

a FIN Packets of a selected variable size or a FIN packet without the ACK or SYN flag properly set; and

a generic, well-formed ICMP ECHO request packet;

a generic well-formed TCP Header set to 1024 bytes in size;

a Packet requesting an ICMP Timestamp;

a Packet with min/max segment size set to a selected variable value; and

a UDP packet with the fragment bit set;

a TCP Packet with the header and options set incorrectly;

a well-formed ICMP Packet;

a Fragmented TCP or UDP packet;

a packet with an empty TCP window or a window set to zero;

a generic TCP Packet with 8K of random data; and

a SYN Packet with ACK and RST flags set.

30-43. (Cancelled)

44. (Currently amended) A method of examining a network, including:

identifying an operating system of a remote host, including a version and a patch level of the operating system with a first set of packets, the first set of packets comprising at least an operating system packet to determine the operating system, an operating system version packet to determine the operating system version based on the determined operating system, and an operating system patch level packet to determine the operating system patch level based on the determined operating system version;

identifying a service of the remote host, including a version and a patch level of the service with a second set of packets based on the identified operating system, the second [[first]] set of packets comprising at least a service packet to determine the service, a service version packet to determine the service version based on the determined service, and a service patch level packet to determine the service patch level based on the determined service version; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

45. (Cancelled)

46. (Currently amended) The method of claim 44 [[1]], wherein identifying a service comprises directing [[the]] communications to ports of the remote host based on the identified operating system.

49. (Cancelled)

Allowable Subject Matter

6. Claims 2, 29, 44 and 46-48 are allowed.

The following is an examiner's statement of reasons for allowance:

Independent claims 29 and 44, of the current application, are directed towards a method that reliably and non-intrusively identifies various conditions of a network. In particular, the invention can identify an operating system, including version and patch level, and a service, including version and patch level, of a remote host on a network. Using this information, the invention can then reliably identify a vulnerability condition of the network. In some

embodiments of the invention, the operating system and service information can be used to identify a Trojan application, unlicensed software use, security policy violations, or even infer vulnerabilities that are yet unknown.

The closest prior art to the current application is Reshef et al U.S. Patent No. 6,584,569 B2 (hereinafter Reshef). Reshef's invention seeks to provide a scanner for automatically detecting potential application-level vulnerabilities or security flaws in a web application. In the web environment, generally speaking, the application scanner analyzes the messages that flow (or would ordinarily flow) between a client browser and a server hosting the web application in order to discover the structure or elements of the application's interface with external clients. Then, based on a pre-defined set of hacking rules or techniques, the scanner mutates client requests in various ways, thereby generating exploits that will be unique for each web application. These exploits may then be used to attack the web application. The attack is monitored and the results evaluated and reported to the user. Reshef discloses long-shot vulnerabilities that are security flaws that generally exist within web servers, application servers and other applications interacting with client browsers. The vulnerabilities are published by a large number of organizations (e.g. BugTraq by SecurePoint.COM, Security Focus) and can be accessed by anybody with Internet access. After the hacker checks the vulnerabilities, he or she can scan through a web site trying to find places where the vulnerability has not been blocked or a patch has not been applied. Reshef discloses a scanner that maintains an updated list of known vulnerabilities in the long shot rules. During the mutation phase the scanner enumerates the relevant vulnerabilities according to the type of web server, application server and other third party applications identified by the operator, thus verifying that the known holes in the system

are blocked. The scanner preferably includes an expert knowledge base for providing advice upon ways of correcting the security flaws exposed by the mutated requests. The suggestions made by knowledge base comprise changes to the site's software or available patches to the problem in cases of third-party platforms. Pressing the "report" icon in FIG. 7 preferably triggers this. Reshef also discloses finding vulnerabilities within an operating system.

However, there are differences between the current application and Reshef. Reshef does not does not teach identifying a version and a patch level of the operating system. Reshef does not teach identifying a service level of the remote host that includes a version and a patch level. Finally, Reshef does not teach identifying a vulnerability of the network based on the information obtained from the steps of identifying the operating system and identifying a service. For these reasons stated, the examiner has allowed independent claims 29 and 44.

Any claims not directly addressed are allowed on the virtue of their dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
March 15, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
3/17/06